

**THAT WHICH IS CLAIMED IS:**

1. A secure wireless local area network (LAN) device comprising:

a housing;

a wireless transceiver carried by said housing;

5 a media access controller (MAC) carried by said housing; and

a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver, said cryptography circuit operating using cryptography  
10 information and rendering unuseable the cryptography information based upon tampering.

2. A secure wireless LAN device according to Claim 1 wherein said cryptography circuit comprises:

at least one volatile memory for storing the cryptography information; and

5 a battery for maintaining the cryptography information in said at least one volatile memory.

3. A secure wireless LAN device according to Claim 2 wherein said cryptography circuit further comprises at least one switch operatively connected to said housing for disconnecting said battery from said  
5 at least one volatile memory so that the cryptography information therein is lost based upon breach of said housing.

4. A secure wireless LAN device according to Claim 1 wherein said cryptographic information comprises a cryptography key.

094673-014604

5. A secure wireless LAN device according to Claim 1 wherein said security information comprises at least a portion of a cryptography algorithm.

6. A secure wireless LAN device according to Claim 1 wherein said MAC implements a predetermined wireless LAN MAC protocol.

7. A secure wireless LAN device according to Claim 6 wherein said predetermined wireless LAN MAC protocol is based upon the IEEE 802.11 standard.

8. A secure wireless LAN device according to Claim 1 further comprising at least one connector carried by said housing for connecting to at least one of a user station and an access point.

9. A secure wireless LAN device according to Claim 8 wherein said at least one connector comprises a PCMCIA connector.

10. A secure wireless LAN device according to Claim 1 wherein said cryptography circuit comprises:  
a cryptography processor; and

a control and gateway circuit connecting said  
5 cryptography processor to said MAC and said wireless transceiver.

11. A secure wireless LAN device according to Claim 1 wherein said wireless transceiver comprises:  
a baseband processor;

a modem connected to said baseband processor; and  
5 a radio frequency transmitter and receiver connected to said modem.

097E3173-044604

12. A secure wireless LAN device according to Claim 1 further comprising at least one antenna carried by said housing and connected to said wireless transceiver.

13. A secure wireless local area network (LAN) device comprising:

a housing;

a wireless transceiver carried by said housing;

5 at least one connector carried by said housing for connecting to at least one of a LAN station and a LAN access point; and

a cryptography circuit carried by said housing and connected to said wireless transceiver, said  
10 cryptography circuit operating using cryptography information and rendering unuseable the cryptography information based upon tampering.

14. A secure wireless LAN device according to Claim 13 wherein said cryptography circuit comprises:

at least one volatile memory for storing the cryptography information; and

5 a battery for maintaining the cryptography information in said at least one volatile memory.

15. A secure wireless LAN device according to Claim 14 wherein said cryptography circuit further comprises at least one switch operatively connected to said housing for disconnecting said battery from said  
5 at least one volatile memory so that the cryptography information therein is lost based upon breach of said housing.

16. A secure wireless LAN device according to Claim 13 wherein said cryptographic information comprises a cryptography key.

17. A secure wireless LAN device according to Claim 13 wherein said security information comprises at least a portion of a cryptography algorithm.

18. A secure wireless LAN device according to Claim 13 further comprising a media access controller (MAC) carried by said housing; and wherein said MAC implements a predetermined wireless LAN MAC protocol.

19. A secure wireless LAN device according to Claim 18 wherein said predetermined wireless LAN MAC protocol is based upon the IEEE 802.11 standard.

20. A secure wireless LAN device according to Claim 13 wherein said at least one connector comprises a PCMCIA connector.

21. A secure wireless LAN device according to Claim 13 wherein said cryptography circuit comprises:  
a cryptography processor; and  
a control and gateway circuit connecting said  
5 cryptography processor to said MAC and said wireless transceiver.

22. A secure wireless LAN device according to Claim 13 wherein said wireless transceiver comprises:  
a baseband processor;  
a modem connected to said baseband processor; and  
5 a radio frequency transmitter and receiver connected to said modem.

23. A secure wireless LAN device according to Claim 13 further comprising at least one antenna carried by said housing and connected to said wireless transceiver.

24. A secure wireless local area network (LAN) device comprising:

a housing;

a wireless transceiver carried by said housing;

5 a media access controller (MAC) carried by said housing; and

a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver, said cryptography circuit comprising

10 at least one volatile memory for storing the cryptography information, and

a battery for maintaining the cryptography information in said at least one volatile memory.

25. A secure wireless LAN device according to Claim 24 wherein said cryptography circuit further comprises at least one switch operatively connected to said housing for disconnecting said battery from said  
5 at least one volatile memory so that the cryptography information therein is lost based upon a breach of said housing.

26. A secure wireless LAN device according to Claim 24 wherein said cryptographic information comprises a cryptography key.

27. A secure wireless LAN device according to Claim 24 wherein said security information comprises at least a portion of a cryptography algorithm.

09763379.011604

28. A secure wireless LAN device according to Claim 24 wherein said MAC implements a predetermined wireless LAN MAC protocol.

29. A secure wireless LAN device according to Claim 28 wherein said predetermined wireless LAN MAC protocol is based upon the IEEE 802.11 standard.

30. A secure wireless local area network (LAN) device comprising:

a housing;

a wireless transceiver carried by said housing;

5 at least one connector carried by said housing for connecting to at least one of a LAN station and a LAN access point; and

a cryptography circuit carried by said housing and connected to said wireless transceiver, said

10 cryptography circuit comprising

at least one volatile memory for storing the cryptography information, and

a battery for maintaining the cryptography information in said at least one volatile memory.

31. A secure wireless LAN device according to Claim 30 wherein said cryptography circuit further comprises at least one switch operatively connected to said housing for disconnecting said battery from said  
5 at least one volatile memory so that the cryptography information therein is lost based upon breach of said housing.

32. A secure wireless LAN device according to Claim 30 wherein said cryptographic information comprises a cryptography key.

0976473 "044604

33. A secure wireless LAN device according to Claim 30 wherein said security information comprises at least a portion of a cryptography algorithm.

34. A secure wireless LAN device according to Claim 30 further comprising a media access controller (MAC) carried by said housing; and wherein said MAC implements a predetermined wireless LAN MAC protocol.

35. A secure wireless LAN device according to Claim 34 wherein said predetermined wireless LAN MAC protocol is based upon the IEEE 802.11 standard.

36. A secure wireless local area network (LAN) system comprising:

a plurality of LAN devices;

5 a respective secure wireless LAN device connected to each of said plurality of LAN devices, each secure wireless LAN device comprising

a housing,

a wireless transceiver carried by said housing, and

10 a cryptography circuit carried by said housing and connected to said wireless transceiver, said cryptography circuit operating using cryptography information and rendering unuseable the cryptography information based upon  
15 tampering.

37. A secure wireless LAN system according to Claim 36 wherein said cryptography circuit comprises:

at least one volatile memory for storing the cryptography information; and

5 a battery for maintaining the cryptography information in said at least one volatile memory.

38. A secure wireless LAN system according to Claim 37 wherein said cryptography circuit further comprises at least one switch operatively connected to said housing for disconnecting said battery from said  
5 at least one volatile memory so that the cryptography information therein is lost based upon breach of said housing.

39. A secure wireless LAN system according to Claim 36 wherein said cryptographic information comprises a cryptography key.

40. A secure wireless LAN system according to Claim 36 wherein said security information comprises at least a portion of a cryptography algorithm.

41. A secure wireless LAN system according to Claim 36 wherein said secure wireless LAN device comprises a media access controller (MAC) connected to said wireless transceiver; and wherein said MAC  
5 implements a predetermined wireless LAN MAC protocol.

42. A secure wireless LAN system according to Claim 41 wherein said predetermined wireless LAN MAC protocol is based upon the IEEE 802.11 standard.

43. A secure wireless LAN system according to Claim 36 wherein said plurality of LAN devices comprises a plurality of user stations.

44. A secure wireless LAN system according to Claim 36 wherein said plurality of LAN devices comprises at least one user station and at least one access point.

096643 0160



45. A secure wireless LAN system according to Claim 36 wherein said plurality of LAN devices comprises a plurality of access points.

46. A method for making tamper resistant a secure wireless local area network (LAN) device comprising a housing, a wireless transceiver carried by the housing and a cryptography circuit carried by the housing, the  
5 method comprising:

storing cryptography information in the cryptography circuit; and

rendering unuseable the cryptography information based upon tampering with the secure wireless LAN  
10 device.

47. A method according to Claim 46 wherein the cryptography circuit comprises at least one volatile memory for storing the cryptography information, and a battery for maintaining the cryptography information in  
5 the at least one volatile memory; and wherein rendering unuseable comprises disconnecting the battery from the at least one volatile memory based upon a breach of the housing.

48. A method according to Claim 46 wherein the cryptographic information comprises a cryptography key.

49. A method according to Claim 46 wherein the security information comprises at least a portion of a cryptography algorithm.

50. A method according to Claim 46 wherein the secure wireless LAN device further comprises a media access controller (MAC) carried by the housing; and

0976470101601

wherein the MAC implements a predetermined wireless LAN  
5 MAC protocol.

51. A method according to Claim 50 wherein the  
predetermined wireless LAN MAC protocol is based upon  
the IEEE 802.11 standard.

09/07/01 01:00